Math 361 lecture for Monday, Week 12

Dirichlet's unit theorem

Let $K$ be a number field, and let $\mathfrak{O}_K^*$ denote the units in $\mathfrak{O}_K$.

**Example 1.**

- We have $\pm 1 \in \mathfrak{O}_K^*$ for all $K$.
- If $K = \mathbb{Q}(i)$, then $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$.
- If $K = \mathbb{Q}(\sqrt{2})$, then $1 + \sqrt{2} \in \mathfrak{O}_K^*$, and $|1 + \sqrt{2}| > 1$. So $\{(1 + \sqrt{2})^k : k \in \mathbb{Z}_{>0}\}$ is an infinite collection of units in $\mathfrak{O}_K^*$.

**Remarks 2.**

(a) $\mathfrak{O}_K^*$ is a multiplicative group.

(b) An element $u \in \mathfrak{O}_K$ is a unit if and only if $N(u) = \pm 1$. (Reminder: If $N(u) = \prod_{i=1}^n \sigma_i(u) = \pm 1$ where $\sigma_1 = \mathrm{id}$, then let $v := \prod_{i=2}^n \sigma^i(u)$. We have $v \in \mathfrak{O}_K$ (let $\sigma_i$ act on the minimal polynomial for $u$), and $\pm v$ is the multiplicative inverse of $u$.)

(c) Elements of finite order in $\mathfrak{O}_K^*$ are roots of unity, and every root of unity in $K$ is in $\mathfrak{O}_K^*$. (If $\zeta \in K$ and $\zeta^m = 1$, them $\zeta$ satisfies $x^m - 1$, and hence is an algebraic integer in $K$.)

(d) The elements of $\mathfrak{O}_K$ with finite order form a finite cyclic subgroup of $\mathfrak{O}_K$ of even order.

*Proof.* These elements clearly form a subgroup. For finiteness, note that the mapping $\sigma : K \to \mathbb{L}^{s,t} \simeq \mathbb{R}^n$ maps $\mathfrak{O}_K$ to a lattice in $\mathbb{R}^n$, and the image of $\{\zeta \in K : |\zeta| = 1\}$ maps to a compact set. Finally, since $-1 \in \mathfrak{O}_K$ and has order 2, it follows that 2 divides the order of the subgroup. The proof that any finite subgroup of $K^*$ must be cyclic is similar to that given in Step 1 of the two square theorem the in the notes for Friday, Week 10. □

**Example 3.** Let $K$ be a cubic number field, i.e., $[K : \mathbb{Q}] = 3$. Let $\zeta$ be a root of unity in $K$. We claim that $\zeta = \pm 1$. Since $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq K$, we have

$$3 = [K : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : K].$$

Therefore, either $\mathbb{Q}(\zeta) = \mathbb{Q}$, in which case $\zeta = \pm 1$, or $K = \mathbb{Q}(\zeta)$. We now show that the case $K = \mathbb{Q}(\zeta)$ is not possible. This is due to that fact (not proven here) that if $\zeta$ is a $k$-th root of unity, then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(k)$, where $\phi$ is the Euler phi-function. However, $\phi$ never takes the value 3. For $k \geq 3$, we have that $\phi(k)$ is even, and $\phi(1) = \phi(2) = 1$. So the only units in a cubic number are $\pm 1$.

**Theorem 4** (Dirichlet's unit theorem)**.** Let $K$ have $s$ real embeddings and $t$ complex embeddings. Then, we have a group isomorphism

$$\mathfrak{O}_K^* \simeq W \times \mathbb{Z}^{s+t-1}$$

where $W$ is the finite cyclic group of roots of unity in $K$ (the subgroup of $\mathfrak{O}_K$ of elements of finite order).

*Proof.* See our text, Appendix B for a full proof. For the idea of the proof, consider the mapping $\ell\colon \mathfrak{O}_K^* \to \mathbb{R}^{s+t}$ which is our usual mapping $\sigma\colon K \to \mathbb{L}^{s,t} = \mathbb{R}^s \times \mathbb{C}^t$, restricted to $\mathfrak{O}_K^*$, followed by the mapping

$$\begin{aligned} \mathbb{R}^s \times \mathbb{C}^t &\to \mathbb{R}^{s+t} \\ (x_1, \ldots, x_s, z_1, \ldots, z_t) &\mapsto (\ln|x_1|, \ldots, \ln|x_s|, \ln|z_1|^2, \ldots, \ln|z_t|^2). \end{aligned}$$

Note that due to the logs, the mapping $\ell$ takes a multiplicative group into and additive subgroup of $\mathbb{R}^n$. One may show that the image of $\ell$ is a lattice of dimension $s+t-1$, and the kernel of $\ell$ is the set of elements of $\mathfrak{O}_K^*$ of finite order. Thus, $\ell$ induces an isomorphism of $\mathfrak{O}_K^*/W$ with a lattice of rank $s+t-1$. It follows from the structure theorem for finitely generated abelian groups that

$$\mathfrak{O}_K^* \simeq W \times \mathbb{Z}^{s+t-1}.$$

To see that the $W \subseteq \ker(\ell)$, first take $\zeta \in W$. Say $\zeta^m = 1$ with $m \geq 1$. Then

$$0 = \ell(1) = \ell(\zeta^m) = m\ell(\zeta).$$

Hence, $\zeta \in \ker(\ell)$. The opposite inclusion requires a bit more work (see our text).

It is also straightforward to see that the image of $\ell$ lies in a lattice of rank at most $s+t-1$. Let $\alpha \in \mathfrak{O}_K^*$. Then

$$\ell(\alpha) = (\ell_1(\alpha), \ldots, \ell_{s+t}(\alpha))$$

where

$$\ell_j = \begin{cases} \ln(|\sigma_j(\alpha)|) & \text{for } 1 \leq j \leq s \\ \ln(|\sigma_j(\alpha)|^2) & \text{for } s+1 \leq j \leq s+t. \end{cases}$$

Therefore,

$$\begin{aligned} 0 &= \sum_{j=1}^{s+t} \ell_j(\alpha) \\ &= \sum_{j=1}^{s} \ln|\sigma_j(\alpha)| + \sum_{j=s+1}^{s+t} \ln|\sigma_j(\alpha)|^2 \\ &= \ln|N(\alpha)| \\ &= 0, \end{aligned}$$

since the norm of a unit is $\pm 1$. We see that the image of $\ell$ sits in the set $\{x \in \mathbb{R}^{s+t} : x_1 + \cdots + x_{s+t} = 0\}$. □

**Remark 5.** The finite group $W$ consists of the roots of unity of $K$. The only real roots of unity are $\pm 1$. Since field embeddings preserve roots of 1, including their orders, it follows that if $K$ has any real embeddings, then $W = \{-1, 1\}$.